(12) INTERNATIONAL AP ATION PUBLISHED UNDER THE PATENT PERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 April 2001 (12.04.2001)

PCT

(10) International Publication Number
WO 01/26322 A3

(51) International Patent Classification[7]: H04L 9/08, 29/06, 12/28

(21) International Application Number: PCT/US00/27352

(22) International Filing Date: 4 October 2000 (04.10.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/157,818 5 October 1999 (05.10.1999) US

(71) Applicant *(for all designated States except US)*: **NORTEL NETWORKS LIMITED** [CA/CA]; World Trade Center of Montreal, 8th Floor, 380 St. Antoine Street West, Montreal, Quebec H2Y 3Y4 (CA).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **KHALIL, Mohamed** [US/US]; 9221 Amberton, Number 180, Dallas, TX 75243 (US). **NARAYANAN, Raja, P.** [IN/US]; 4713 N. O'Connor Road, Apt. 1026, Irving, TX 75062 (US). **AKHTAR, Haseeb** [US/US]; 3102 Pamela Place, Garland, TX 75044 (US). **QADDOURA, Emad, A.** [US/US]; 1320 Wateredge Drive, Plano, TX 75093 (US).

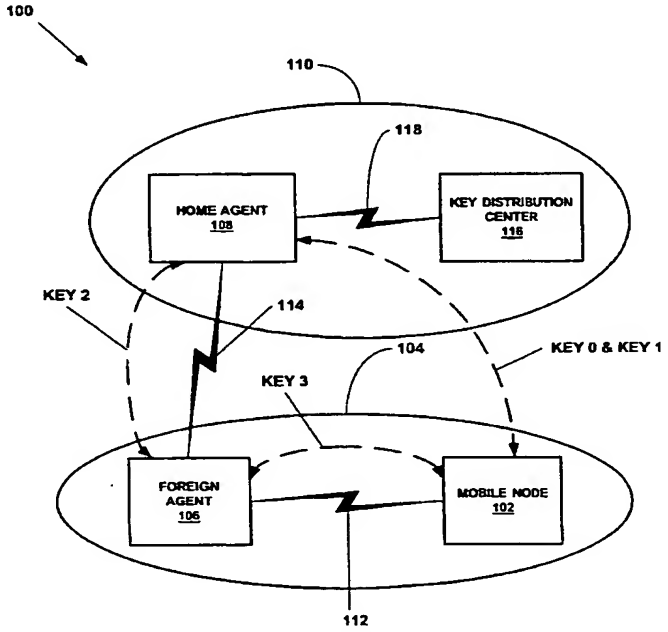
(74) Agents: **MCCOMBS, David, L.**; Haynes and Boone, L.L.P., 901 Main Street, Suite 3100, Dallas, TX 75202-3789 et al. (US).

(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: KEY EXCHANGE FOR A NETWORK ARCHITECTURE



(57) Abstract: A key exchange for a network architecture. A mobile node that roams over a foreign domain transmits a registration request to a home domain using the foreign domain. The identity of the mobile node within the registration request is encrypted. The home domain receives the registration request and decrypts the mobile node identity. The home domain generates a registration reply that includes encryption keys for encrypting information to be transmitted between and among the home domain, the foreign domain, and the mobile node.

WO 01/26322 A3

Published:
— *with international search report*

(88) Date of publication of the international search report:
8 November 2001

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

Int[illegible]ional Application No
P[illegible]S 00/27352

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/08 H04L29/06 H04L12/28

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	YAIR FRANKEL ET AL: "SECURITY ISSUES IN A CDPD WIRELESS NETWORK" IEEE PERSONAL COMMUNICATIONS,US,IEEE COMMUNICATIONS SOCIETY, vol. 2, no. 4, 1 August 1995 (1995-08-01), pages 16-27, XP000517586 ISSN: 1070-9916	1,16,31, 45-49
A	page 20, right-hand column, line 17 -page 23, line 50	2-15, 17-30, 32-44, 50-127
A	EP 0 912 026 A (LUCENT TECHNOLOGIES INC) 28 April 1999 (1999-04-28) page 16, line 5 - line 44 page 20, line 16 -page 23, line 20	1-127

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 April 2001	17/05/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Meurisse, W

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

[redacted] International Application No
P[redacted]S 00/27352

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	JACOBS S ET AL: "SECURITY OF CURRENT MOBILE IP SOLUTIONS" NOV. 3 - 5, 1997,NEW YORK, NY: IEEE,US, 3 November 1997 (1997-11-03), pages 1122-1128, XP000792591 ISBN: 0-7803-4250-X	64,70, 76,82, 98-100, 106,109, 116,120, 124
A	page 1125, left-hand column, paragraph 3 -page 1127, right-hand column, paragraph 5	1-63, 65-69, 71-75, 77-81, 83-97, 101-105, 107,108, 110-115, 117-119, 121-123, 125-127

A	JORDAN F ET AL: "SECURE MULTICAST COMMUNICATIONS USING A KEY DISTRIBUTION CENTER" PROCEEDINGS OF THE IFIP TC6 INTERNATIONAL CONFERENCE ON INFORMATION NETWORKS AND DATA COMMUNICATION, FUNCHAL, MADEIRA ISLAND, PORTUGAL, APR. 18 - 21, 1994,AMSTERDAM, NORTH HOLLAND,NL, vol. CONF. 5, 18 April 1994 (1994-04-18), pages 367-380, XP000593303 ISBN: 0-444-81869-3 the whole document	1-127

A	RICHARD E. SMITH: "Internet Cryptography" October 1997 (1997-10) , ADDISON-WESLEY , USA/CANADA XP002165437 page 120 -page 121 page 200 -page 203	1-127

A	HARKINS,CARREL: "The Internet Key Exchange (IKE)" NETWORK WORKING GROUP RFC 2409, INTERNET ENGINEERING TASK FORCE(IETF) STANDARDS TRACK, November 1998 (1998-11), XP002165435 page 12, paragraph 5.2 -page 19, last line	1-127

X	MAUGHAN, SCHERTLER, SCHNEIDER, TURNER: "Network Working roup RFC 2408 Standards Track" INTERNET SECURITY ASSOCIATION AND KEY MANAGEMENT PROTOCOL (ISAKMP), November 1998 (1998-11), XP002165436	88
A	page 27, paragraph 3.4 -page 31, last line page 44, paragraph 4 -page 54, paragraph 4.6	1-87, 89-127

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 00/27352

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0912026 A	28-04-1999	CA 2249817 A	14-04-1999
		CA 2249830 A	14-04-1999
		CA 2249831 A	14-04-1999
		CA 2249836 A	14-04-1999
		CA 2249837 A	14-04-1999
		CA 2249838 A	14-04-1999
		CA 2249839 A	14-04-1999
		CA 2249862 A	14-04-1999
		CA 2249863 A	14-04-1999
		EP 0910198 A	21-04-1999
		EP 0917320 A	19-05-1999
		EP 0917318 A	19-05-1999
		EP 0912027 A	28-04-1999
		EP 0912012 A	28-04-1999
		EP 0917328 A	19-05-1999
		EP 0918417 A	26-05-1999
		EP 0912017 A	28-04-1999
		JP 11289353 A	19-10-1999
		JP 11252183 A	17-09-1999
		JP 11275154 A	08-10-1999
		JP 11275155 A	08-10-1999
		JP 2000022758 A	21-01-2000
		JP 11275156 A	08-10-1999
		JP 11275157 A	08-10-1999
		JP 11284666 A	15-10-1999
		JP 11331276 A	30-11-1999